PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | |
|---|---|
| **In Re Application of**<br><br>**Mitchell B. OLIVER, et al.**<br><br>**Serial No. 10/791,160**<br><br>**Filed: March 1, 2004** | **EXECUTION OF UNVERIFIED PROGRAMS IN A WIRELESS DEVICE OPERTING ENVIRONMENT**<br>**EXPEDITED PROCEDURE**<br>**EXAMINING GROUP 2451**<br><br>**Group No. 2451** |

**BRIEF ON APPEAL UNDER 37 C.F.R. § 41.37**

MS Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 223 13-1450

Sir:

In response to the Final Office Action dated October 7, 2009 and the Advisory Action dated January 7, 2010, the Appellants on February 11, 2010 requested an Appeal to consider the issues raised or maintained in the Final Office Action. Accordingly, this Brief on Appeal under 37 C.F.R. §41.37 is being filed.

The fees required under § 41.20(b)(2) should be charged to Deposit Account No. 17-0026.

## TABLE OF CONTENTS

## I. Real Party in Interest

The real party in interest in this appeal is QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, California, 92121.

## II. Related Appeals and Interferences

To the best of Appellants' knowledge, there are no other previous or pending appeals of this Application, or patent interference proceedings, or judicial proceedings which may be related to, directly affect, or be directly affected by, or have a bearing on the Board's decision of this Appeal.

## III. Status of Claims

Claims 1-24 are on Appeal, with claims 1, 10, 11, 18, and 19 being independent.

1. Claims cancelled: none.
2. Claims withdrawn from consideration but not cancelled: none
3. Claims pending: 1-24.
4. Claims allowed: none.
5. Claims rejected: 1-24.

## IV. Status of Amendments

The Amendments made in the Appellants' response filed on 12/04/2009 were entered by the Examiner as indicated on the continuation sheet (PTOL-303) of the 1/07/2010 Advisory Action. Accordingly, there are no un-entered amendments.

## V. Summary of the Claimed Subject Matter

Independent claim 1 is directed to a computer device **(e.g., 10 of FIGS. 1 and/or 2, see Page 4, line 26 to Page 7, line 18)** having wireless communication capability, including a wireless communication portal **(e.g., 24 of FIG. 1, see Page 5, lines 19-21)** for selectively sending and receiving data across a wireless network **(e.g., 25 of FIG. 1, see Page 5, lines 19-21)**, a computer platform **(e.g., 12 of FIG. 1, see Page 4, line 26 to Page 5, line 5)** including a resident application environment **(e.g., 16 of FIG. 1, see Page 4, line 26 to Page 5, line 5)** configured to selectively download applications to the platform through the portal, the resident application environment configured to selectively download applications that comply with predefined security protocol **(e.g., 64-66 of FIG. 4, see Page 9, lines 14-34)**, a data store **(e.g., 12 and/or 20 of FIG. 1, see Page 5, lines 19-31)** in communication with the computer platform and selectively sending data to and receiving data from the computer platform and a download manager **(e.g., 18 of FIG. 1, see Page 4, line 34 to Page 5, line 5 and/or Page 5, lines 26-30)** resident on the computer platform that is configured to selectively download applications through the portal that do not comply with the predefined security protocol **(e.g., 64, 68 and 70 of FIG. 4, see Page 9, lines 14-34)**.

Independent claim 10 is directed to a computer device **(e.g., 10 of FIGS. 1 and/or 2, see Page 4, line 26 to Page 7, line 18)** having wireless communication capability, including a wireless communication means **(e.g., 24 of FIG. 1, see Page 5, lines 19-21)** for selectively sending and receiving data across a wireless network **(e.g., 25 of FIG. 1, see Page 5, lines 19-21)**, a computer means **(e.g., 12 and 16 of FIG. 1, see Page 4, line 26 to Page 5, line 5)** selectively downloading applications through the wireless communication means, the computer means configured to selectively download applications that comply with a predefined security protocol **(e.g., 64-66 of FIG. 4, see Page 9, lines 14-34)** and a means **(e.g., 18 of FIG. 1, see**

**Page 4, line 34 to Page 5, line 5 and/or Page 5, lines 26-30)** for selectively downloading applications through the wireless communication means that do not comply with the predefined security protocol **(e.g., 64, 68 and 70 of FIG. 4, see Page 9, lines 14-34)**.

Independent claim 11 is directed to a method of selectively downloading through a wireless connection to a computer device **(e.g., 10 of FIGS. 1 and/or 2, see Page 4, line 26 to Page 7, line 18)** an application that does not comply with a predefined security protocol for use at that computer device, including the steps of downloading **(e.g., 64, 68 and 70 of FIG. 4, see Page 9, lines 14-34)**, from a wireless network **(e.g., 25 of FIG. 1, see Page 5, lines 19-21)** to a computer platform **(e.g., 12 of FIG. 1, see Page 4, line 26 to Page 5, line 5)** of the computer device, an application that does not comply with a predefined security protocol for use at that computer device, the computer platform including a resident application environment **(e.g., 16 of FIG. 1, see Page 4, line 26 to Page 5, line 5)** for downloading and executing applications **(e.g., 64-66 of FIG. 4, see Page 9, lines 14-34)** utilizing a predefined security protocol for at least downloading an application, the downloading of the non-complying application occurring through the use of a download manager **(e.g., 18 of FIG. 1, see Page 4, line 34 to Page 5, line 5 and/or Page 5, lines 26-30)** resident on the computer platform and executing **(e.g., 74, 78 and 80 of FIG. 4, see Page 10, lines 1-9)** the application at the computer device with the download manager.

Independent claim 18 is directed to a method of selectively downloading through a wireless connection to a computer device **(e.g., 10 of FIGS. 1 and/or 2, see Page 4, line 26 to Page 7, line 18)** an application that does not comply with a predefined security protocol for use at that computer device, including a step for downloading **(e.g., 64, 68 and 70 of FIG. 4, see Page 9, lines 14-34)**, through the wireless connection to a computer platform **(e.g., 12 of FIG. 1, see Page 4, line 26 to Page 5, line 5)** of the computer device, an application that does not

comply with a predefined security protocol for use within a resident application environment **(e.g., 16 of FIG. 1, see Page 4, line 26 to Page 5, line 5)** at that computer device and a step for executing **(e.g., 74, 78 and 80 of FIG. 4, see Page 10, lines 1-9)** the downloaded application at the computer device outside of the resident application environment **(e.g., 74, 78 and 80 of FIG. 4, see Page 10, lines 1-9)**.

Independent claim 19 is directed to, in a computer-readable storage medium **(e.g., 20 of FIG. 1, see Page 11, lines 1-11)**, a program that when executed by a wireless computer device **(e.g., 10 of FIGS. 1 and/or 2, see Page 4, line 26 to Page 7, line 18)** causes the device to perform the steps of downloading **(e.g., 64, 68 and 70 of FIG. 4, see Page 9, lines 14-34)** through a wireless connection to a computer platform **(e.g., 12 of FIG. 1, see Page 4, line 26 to Page 5, line 5)** of the computer device an application that does not comply with a predefined security protocol for use at that computer device, the computer platform including a resident application environment **(e.g., 16 of FIG. 1, see Page 4, line 26 to Page 5, line 5)** for downloading and executing applications utilizing a predefined security protocol **(e.g., 64-66 of FIG. 4, see Page 9, lines 14-34)** for at least downloading an application, the downloading occurring through the use of a download manager **(e.g., 18 of FIG. 1, see Page 4, line 34 to Page 5, line 5 and/or Page 5, lines 26-30)** on the computer platform and executing **(e.g., 74, 78 and 80 of FIG. 4, see Page 10, lines 1-9)**the application at the computer device with the download manager.

## VI. Grounds of Rejection to be Reviewed on Appeal

In the 10/07/2009 Final Rejection, the Office finally rejected:

(1) Claims 11-21 under 35 U.S.C. § 102(e) as being allegedly anticipated by U.S. Publication No. 2005/0033969 ("Kiiveri"); and

(2) Claims 1-10 and 22-24 under 35 U.S.C. § 103(a) as being allegedly unpatentable over U.S. Publication No. 2004/0220998 ("Shenfield") in view of Kiiveri.

## VII. Argument

### (1) Regarding the Rejection of Claims 11-21 under 35 U.S.C. § 102(e) over Kiiveri.

*1. Discussion of Kiiveri.*

Kiiveri is directed to a secure execution architecture, where secure environment hardware is kept physically separate from memory that stores potentially unsecure applications (e.g., see FIG. 1 of Kiiveri). The CPU illustrated in FIG. 1 operates either in secure mode or unsecure mode (e.g., see FIG. 2 of Kiiveri). The mode of the CPU is controlled by a security control register within the secure environment hardware, with respect to which Kiiveri states that "[t]he purpose of the security control register is to give the CPU access to the secure environment, or prevent the CPU from accessing the secure environment, depending on the mode set in the register" (e.g., see [0025] of Kiiveri). Kiiveri states that "[i]n the secure mode, the processor has access to security related data located within the secure environment" (e.g., see [0030] of Kiiveri), and that "if … unsecure mode is activated … [t]he secure environment is now inaccessible" (e.g., see [0032] of Kiiveri).

With respect to FIG. 2 of Kiiveri, Kiiveri discloses that "signatures for the first protected application and operating system to be downloaded are checked", "[i]f the signatures are correct, the application and the operating system is downloaded into the secure environment RAM", and "if the signature check fails or if no signature is present, unsecure mode is activated and the non-

verified application is loaded into the ASIC RAM located outside the secure environment" (e.g., see [0031]-[0032] of Kiiveri).

2. *The Office has incorrectly interpreted a download of an application over a wireless connection as claimed as a selective loading of memory at a computer device during boot-up in Kiiveri.*

As shown in FIG. 1 of Kiiveri, a boot application is stored in a boot read-only-memory (ROM) within a secure portion of an ASIC. When the ASIC powers-up, the boot application copies an operating system (OS) and other application software into either a 'secure' RAM or into an unsecure RAM (referred to as 'ASIC RAM') which is in an unsecure portion of the ASIC. In particular, Kiiveri states "[t]he secure environment comprises a ROM from which the ASIC is booted. This ROM contains boot application software and an operating system OS", and that "by controlling this boot software, it is also possible to control the initial activation of every terminal" (e.g., see [0022]-[0023] of Kiiveri).

Basically, during power-up of the ASIC, a unique key (e.g., which is 'fused' into the ASIC and cannot change, see [0025] of Kiiveri) is used to determine whether to load software into the secure RAM or the ASIC RAM. With respect to FIG. 2 of Kiiveri, Kiiveri states that "[a]t power up, ROM boot software activates secure mode for initial configuration," after which "signatures for the first protected application and operating system to be downloaded are checked" (e.g., see [0031] of Kiiveri). In other words, the applications and/or OS stored in the boot ROM are checked to determine whether they are properly encoded with the unique key.

Kiiveri then states that "[i]f the signatures are correct, the application and the operating system is **downloaded** into the secure environment RAM" and that "[w]hen the desired software has been downloaded, the CPU is informed that the download is completed and the CPU starts executing the verified software" (e.g., see [0031] of Kiiveri, Emphasis added). In context, the Appellants believe that the term "downloading" in Kiiveri is used interchangeably with what

would more normally be referred to as "loading." Indeed, in the next paragraph, Kiiveri states "if the signature check fails or if no signature is present, unsecure mode is activated and the non-verified application is **loaded** into the ASIC RAM" (e.g., see [0032] of Kiiveri, Emphasis added). In the context of Kiiveri, referring to FIG. 1, this type of downloading or loading simply corresponds to the ASIC transferring the OS and application software from the boot ROM into either (i) the secure RAM or (ii) into the ASIC RAM.

By contrast, independent claim 19 (which has not been amended) recites "downloading through a wireless connection to a computer platform of the computer device an application" (Emphasis added). The "downloading" recited in independent claim 19 thereby occurs wirelessly, which implies that the download corresponds to application data being received from a remote or external entity. The alleged 'downloading' in Kiiveri, by contrast, simply corresponds to transferring data from permanent storage (i.e., a ROM) into power-dependent (but more flexible) storage in a RAM (e.g., either an unsecure ASIC RAM or a secure RAM).

Accordingly, Kiiveri's alleged "downloading" is fundamentally different than the downloading being claimed, because Kiiveri's usage of the term "downloading" is somewhat unorthodox and actually relates to a memory transfer between different memory units on the same device (i.e., loading, not 'down'-loading). Also, the transfer of the OS and application software from the boot ROM to either RAM does not occur "through a wireless connection" as claimed.

The Appellants have further made this feature explicit in similar fashion into independent claims 11 and 18 by Amendment during prosecution. For example, independent claim 11 recites that the "downloading" occurs "from a wireless network to a computer platform of the computer device." Again, the power-up loading of memory from the ROM to the RAM in Kiiveri clearly

does not correspond to retrieval of an application from a wireless network. Indeed, requiring ASICs to download their OS during each boot would be incredibly time-consuming.

For the reasons given above, the Appellants respectfully submit that the Office's reading of the "downloading" feature upon the selective loading of data into the secure RAM or non-secure RAM during boot-up is incorrect and should be withdrawn. In the next section, the Appellants will show that when downloading is given a proper interpretation, each of the independent claims rejected in this section distinguish over Kiiveri.

*3. The Office's remarks in the 1/07/2010 Advisory Action do not justify the Office's interpretation of "downloading" in Kiiveri.*

In the 1/07/2010 Advisory Action, the Office maintained its position that the "downloading" referred to by Kiiveri occurs over a wireless connection from an external entity or network. Specifically, the Office stated that "Examiner would like to point out that the PDA operate through wireless connection as known in the art" (e.g., see the Part A of REQUEST FOR CONSIDERATION/OTHER section of the 1/09/2010 Advisory Action). The Appellants are not disputing that the computing device of Kiiveri, which can be a PDA, is capable of downloading applications wirelessly. However, the Office is reading the "downloading" claim language specifically upon the boot OS being loading into secure or non-secure RAM in Kiiveri, which is not a wireless download. Any wireless downloading performed by Kiiveri's PDA would have to occur after it was properly initialized and booted, as is known in the art. A PDA and other computing devices simply cannot download applications wirelessly before they are booted.

In the 1/07/2010 Advisory Action, the Office also stated that "in paragraph 3 [of Kiiveri], it clearly states mobile telecommunication terminals such as PDA which means the PDA is operating through a wireless connections, since the application and the operating system and is downloaded into the secure environment" (e.g., see the Part A of REQUEST FOR

CONSIDERATION/OTHER section of the 1/09/2010 Advisory Action). Again, the Appellants believe the Office is confusing wireless connectivity available after boot-up with the loading of memory between internal storage areas of the PDA during boot-up.

After discussing the high-level wireless connectivity of Kiiveri's PDA, the Office states that "if the signature check fails … the unsecured mode is activated and the verified application is loaded in ASIC RAM" and "[i]n this case, the loading is done on to ASIC RAM of the mobile PDA, which means that since the PDA operate in mobile environment, it is loaded through wireless connection" (e.g., see the Part A of REQUEST FOR CONSIDERATION/OTHER section of the 1/09/2010 Advisory Action). The Appellants believe this statement captures the very heart of the issue on Appeal. The Office believes that because a PDA can operate in a wireless environment, then its OS is loaded over a wireless connection. The Appellants totally disagree with this conclusion. Wireless devices always include some type of permanent storage so they can begin operating as soon as they are turned-on or booted. Only after wireless devices are booted do they search for wireless pilot signals to obtain a wireless connection. The Office incorrectly assumes that because a PDA is wireless, then all of its memory loading occurs wirelessly. This is simply an inaccurate characterization of electronic devices in general and wireless devices in particular.

4. *When a correct interpretation of "downloading" is applied to Kiiveri, Kiiveri fails to disclose or suggest that a module responsible for downloading an application is selectively responsible or not responsible for executing the downloaded application as claimed.*

As noted above, Kiiveri teaches loading verified applications to a secure environment RAM, and loading non-verified applications to a non-secure RAM. Kiiveri's PDA is still capable of downloading applications after the boot-up. Even under this alternative interpretation of Kiiveri, however, Kiiveri does not appear to disclose or suggest "executing the application at

the computer device with the download manager" as recited in independent claim 11 and similarly recited in independent claims 18 and 19.

The Office cites to Paragraph [0032] of Kiiveri for allegedly disclosing this feature (e.g., see Page 10 of the 10/07/2009 Final Office Action), but the only teaching in this section of Kiiveri related to execution of the non-verified application is that "[w]hen boot is completed, this non-verified application is executed by the CPU." This does not appear to disclose or suggest that the mechanism responsible for downloading the non-verified application is also responsible for its execution as claimed. In other words, a general execution of the non-verified application by the CPU in Kiiveri does not imply that the non-verified application is executed by a download manager that was also used to download the non-verified application in the first place.

Accordingly, the Appellants respectfully submit that Kiiveri cannot disclose or suggest "the downloading of the non-complying application occurring through the use of a download manager resident on the computer platform" and "executing the application at the computer device with the download manager" as recited in independent claim 11 and similarly recited in independent claims 18 and 19.

As such, claims 12-17 and 20-21, dependent upon independent claims 11 and 19, respectively, are likewise allowable over Kiiveri at least by virtue of their dependence upon the independent claims.

The Appellants respectfully request that the Board withdraw this art grounds of rejection.

**(2) Regarding the Rejection of Claims 1-10 and 22-24 under 35 U.S.C. § 103(a) over Shenfield in view of Kiiveri.**

*1. An application server in Shenfield is relied upon for disclosing a "computer platform" as claimed, but the application server does not have "wireless communication capability" as required for the claimed "computer platform".*

Shenfield is directed to a system and method of building wireless component applications (e.g., Shenfield, Abstract). The Office reads the claimed "computer platform" upon the application server (e.g., see Page 3 of the 10/07/2009 Final Office Action, "[t]he reference teaches downloading client application program in relation to the application server (a computer platform)"). Independent claims 1 and 10 are directed to computer devices "having wireless communication capability," and not a more generic "computer device." As such, the Appellants submit that the computer devices of independent claims 1 and 10 cannot read on the application server 110 of Shenfield. With regard to the wireless communication devices actually disclosed by Shenfield (e.g., *mobile communication devices 100 as illustrated in Shenfield at FIG. 1, for example*), the Appellants respectfully submit that Shenfield fails to disclose or suggest the remaining claim features under this interpretation of the claim language.

*2. Discussion of the Office's admitted deficiencies of Shenfield with respect to other claim features, and how Kiiveri does not cure these particular deficiencies.*

Further, the Appellants agree with the Office in that "Shenfield is silent in teaching a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the predefined security protocol" (e.g., see Page 3 of the 10/07/2009 Final Office Action). However, the Office alleges that Kiiveri cures this particular deficiency of Shenfield.

In the preceding section related to the 35 U.S.C. § 102(e) rejection over Kiiveri, the Appellants discussed Kiiveri in great detail and demonstrated that Kiiveri uses the term

"downloading" to refer to the loading of data from permanent memory (i.e., a ROM) into temporary memory (i.e., either a secure RAM or an unsecure ASIC RAM, based an associated application-signature ID). This is clearly not the same as "a download manager resident on the computer platform that is configured to selectively download applications through [a wireless communication] portal" as recited in independent claim 1 and similarly recited in independent claim 10.

As such, claims 2-9 and 22-24, dependent upon independent claim 1, are likewise allowable over Shenfield in view of Kiiveri at least by virtue of their dependence upon the independent claims.

*3. Even if one of ordinary skill in the art combined aspects of Kiiveri with Shenfield, the result would not correspond to the claimed invention.*

The combination alleged by the Office is not supportable from the viewpoint of one skilled in the art. The logical combination of Shenfield and Kiiveri (assuming they would be combinable, which the Appellants do not admit) would be to have the processor and memory architecture of Kiiveri embedded in the wireless device of Shenfield for loading of data from permanent memory (i.e., a ROM) into temporary memory secure RAM or an unsecure ASIC RAM for operation. Since the teachings of Kiiveri are directed to a processor and memory architecture, which are inherent in a wireless device (e.g., 100) of Shenfield, the logical combination of Shenfield and Kiiveri (if one exists) would be to modify the processor and memory architecture of the wireless device of Shenfield to comply with the processor and memory architecture taught by Kiiveri.

Instead of this combination, the Office alleges that Shenfield would be modified such that wireless downloads in Shenfield are affected by Kiiveri's boot-time loading of memory. However, the Appellants once again submit that a process associated with the selective loading

of memory during boot-up or power-up as in Kiiveri would not be carried over into the realm of wireless downloads. The OS is the lowest-layer of operation on virtually any computing device, so security of the OS during boot-up is critical. It is unclear whether the same precautions as applied in Kiiveri at the OS-level would be carried over to mere application downloads, for which devices have other mechanisms of protection. For example, all downloaded applications in Shenfield could be routed to non-secure RAM, such that no signature check need be performed as in Kiiveri.

Accordingly, for at least this additional reason, the Appellants respectfully submit that Kiiveri does not cure Shenfield's admitted deficiency with regard to the above-noted claim limitations of independent claims 1 and/or 10.

The Appellants respectfully request that the Board withdraw this art grounds of rejection.

4. *The Office's remarks in the 1/07/2010 Advisory Action do not justify the Office's particular combination of Kiiveri with Shenfield.*

In the 1/07/2010 Advisory Action, the Office maintained its position that "it would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Kiiveri's teaching in Shenfield's teaching to come up with having downloading application that does not comply security protocol. The motivation for doing so would be so that the testing, debugging and serving the mobile telecommunication" (e.g., see the Part B of REQUEST FOR CONSIDERATION/OTHER section of the 1/09/2010 Advisory Action).

The Appellants believe that the Office is attempting to generalize Kiiveri's boot-up procedure so that its selective secure RAM or non-secure RAM loading feature can be implemented anywhere in any system, such as Shenfield's application-download system. However, the Appellants believe this is taking Kiiveri's teachings out of context.

As discussed in the preceding section, Kiiveri is simply trying to verify that a signature associated with an OS is correct at boot-time so that a device knows whether to operate in secure mode or non-secure mode. Presumably, in Shenfield, when an application is being downloaded to a device, the OS on the device is already being executed. Therefore, Kiiveri's teachings would not be applied at this higher-level of operation in Shenfield.

For at least this additional reason, the Appellants respectfully request that the Board withdraw this art grounds of rejection.

## VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

## IX. EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the Office is being submitted.

## X. RELATED PROCEEDINGS

No related proceedings are referenced in Section II, above.

## XI. CONCLUSION

The Appellants respectfully submit that claims 1-24 are patentable over the applied art and that all of the rejections and objections of record should be reversed.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated April 6, 2010

By: /Fariba Yadegar-Bandari/
Fariba Yadegar-Bandari
Reg. No. 53,805
(858) 651-0397

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Facsimile: (858) 658-2502

## APPENDIX A: CLAIMS

1. (Previously presented) A computer device having wireless communication capability, comprising:

a wireless communication portal for selectively sending and receiving data across a wireless network;

a computer platform including a resident application environment configured to selectively download applications to the platform through the portal, the resident application environment configured to selectively download applications that comply with predefined security protocol;

a data store in communication with the computer platform and selectively sending data to and receiving data from the computer platform; and

a download manager resident on the computer platform that is configured to selectively download applications through the portal that do not comply with the predefined security protocol.

2. (Original) The device of claim 1, wherein the download manager exists within resident application environment and uses an existing application download interface.

3. (Original) The device of claim 1, wherein the downloaded application is immediately executed.

4. (Original) The device of claim 1, wherein a downloaded application that does not comply with the predefined security protocol is stored, and the stored application is executed through the download manager.

5. (Original) The device of claim 1, wherein the download manager further manages executing the downloaded application that does not comply with the predefined security protocol.

6. (Original) The device of claim 4, wherein the download manager further manages storage of the downloaded application that does not comply with the predefined security protocol in the data store.

7. (Original) The device of claim 1, wherein the predefined security protocol is verifying the origination of the application.

8. (Original) The device of claim 1, wherein the predefined security protocol is verifying the presence of a certificate within the downloaded application.

9. (Original) The device of claim 5, wherein the download manager executes the downloaded application that does not comply with the predefined security protocol outside of the resident application environment.

10. (Previously presented) A computer device having wireless communication capability, comprising:

a wireless communication means for selectively sending and receiving data across a wireless network;

a computer means selectively downloading applications through the wireless communication means, the computer means configured to selectively download applications that comply with a predefined security protocol; and

a means for selectively downloading applications through the wireless communication means that do not comply with the predefined security protocol.

11. (Previously presented) A method of selectively downloading through a wireless connection to a computer device an application that does not comply with a predefined security protocol for use at that computer device, comprising the steps of:

downloading, from a wireless network to a computer platform of the computer device, an application that does not comply with a predefined security protocol for use at that computer device, the computer platform including a resident application environment for downloading and executing applications utilizing a predefined security protocol for at least downloading an application, the downloading of the non-complying application occurring through the use of a download manager resident on the computer platform; and

executing the application at the computer device with the download manager.

12. (Original) The method of claim 11, wherein the download manager exists within resident application environment and the step of downloading uses an existing application download interface.

13. (Original) The method of claim 11, further comprising the steps of:

storing, with the download manager, the downloaded application that does not comply with the predefined security protocol; and

executing the stored application through the download manager.

14. (Original) The method of claim 11, further comprising the step of verifying the nature of the downloaded application as the predefined security protocol.

15. (Original) The method of claim 14, wherein the step of verifying the nature of the downloaded application is verifying the presence of a certificate within the downloaded application.

16. (Original) The method of claim 11, wherein the step of executing the downloaded application with the download manager occurs outside of the resident application environment.

17. (Original) The method of claim 11, further comprising the step of downloading the download manager to the computer platform of the computer device after a request to download an application that does not comply with a predefined security protocol has been made, and prior to the step of downloading the requested application.

18. (Previously presented) A method of selectively downloading through a wireless connection to a computer device an application that does not comply with a predefined security protocol for use at that computer device, comprising the steps of:

a step for downloading, through the wireless connection to a computer platform of the computer device, an application that does not comply with a predefined security protocol for use within a resident application environment at that computer device; and

a step for executing the downloaded application at the computer device outside of the resident application environment.

19. (Previously presented) In a computer-readable storage medium, a program that when executed by a wireless computer device causes the device to perform the steps of:

downloading through a wireless connection to a computer platform of the computer device an application that does not comply with a predefined security protocol for use at that computer device, the computer platform including a resident application environment for downloading and executing applications utilizing a predefined security protocol for at least downloading an application, the downloading occurring through the use of a download manager on the computer platform; and

executing the application at the computer device with the download manager.

20. (Original) The program of claim 19, wherein the download manager is resident on the computer platform.

21. (Original) The program of claim 19, wherein the download manager is loaded to the computer platform after a request to download of an application that does not comply with a predefined security protocol and prior to download thereof.

22. (Previously presented) The computer device of claim 1,

wherein the download manager exists within resident application environment and uses an existing application download interface, and

wherein the download manager further manages executing the downloaded application that does not comply with the predefined security protocol.

23. (Previously presented) The computer device of claim 1, wherein the predefined security protocol includes an application validation requirement of the resident application environment.

24. (Previously presented) The computer device of claim 1, wherein the applications being downloaded by the resident application environment in compliance with the predefined security protocol and the applications being downloaded by the download manager in non-compliance with the predefined security protocol are both stored in the data store.

## APPENDIX B: EVIDENCE

(None)

## APPENDIX C: RELATED PROCEEDINGS

(None)